IN THE CLAIMS:

The following is a complete listing of the claims in this application, reflects all changes currently being made to the claims, and replaces all earlier versions and all earlier listings of the claims.

It is noted that the underlining of variables in the following listing of the claims in the originally filed claims and is meant to be permanent.

1. (Currently Amended) A method of encoding over a Galois field F_q, where q is an integer greater than 2 and equal to a power of a prime number, in which a word $\underline{v}' = (v'_0, v'_1, ..., v'_{n'-1})$ is calculated, where $n' \geq 3$, belonging to an [[“MDS”]] MDS linear cyclic code C' of dimension (n'-m), where $1 \leq m \leq n'-2$, on the basis of a word $\underline{a} = (a_0, a_1, ..., a_{n-m-1})$ of information symbols, where $m < n < n'$, ~~characterized in that~~ in which a set $\underline{s} = (s_0, s_1, ..., s_{n-1})$ of strictly increasing integers, with $s_0 \geq 0$ and $s_{n-1} \leq n'-1$, having been predetermined, the method comprising ~~it comprises~~ the ~~following~~ steps of:

a) forming the polynomial $\alpha(x) \equiv \sum_{i=m}^{n-1} a_{i-m} x^{s_i}$,

b) calculating the remainder r(x) of the Euclidean division of a(x) by the polynomial $g(x) \equiv \sum_{p=0}^{m} g_p x^p$ generating said code C',

c) calculating the polynomial

$v*(x) = a(x) - r(x) \equiv \sum_{i=0}^{n'-1} v*_i \, x^i$, corresponding to the word $\underline{v}*=(v*_0, v*_1, ..., v*_{n'-1})$, and

d) taking $\underline{v}' = \underline{v}*$ if $s_{m-1} = m-1$; otherwise obtaining said word $\underline{v}'$ by taking:

$$\underline{v}' = v* + \sum_{j=0}^{s_m-m-1} f_j \underline{\Gamma}^j \qquad (1)$$

in which the words $\underline{\Gamma}^j$ of length n' are defined by: $\Gamma^j_i = g_{i-j}$ for $j \leq i \leq j + m$, and $\Gamma^j_i = 0$ otherwise, and in which the elements f_j of F_q are calculated by means of the equations (1) in which, for the $(s_m - m)$ values of $i < s_m$ not belonging to the set $\underline{s}$, each component v'_i is taken equal to a respective predetermined constant.

2. (Currently Amended) An encoding method according to claim 1, ~~characterized in that it comprises an additional step consisting~~ further comprising the step of deleting said components of predetermined value from $\underline{v}'$, so as to form a word $\underline{v}$ of length n.

3. (Currently Amended) A method of encoding over a Galois field F_q, where q is an integer greater than 2 and equal to a power of a prime number, in which a word $\underline{v}'=(v'_0, v'_1, ..., v'_{n'-1})$ is calculated, where $n' \geq 3$, belonging to an [["MDS"]] MDS linear cyclic code C' of dimension (n'-m), where $1 \leq m \leq n'-2$, on the basis of a word $\underline{a} =(a_0, a_1, ..., a_{n-m-1})$ of information symbols, where $m < n < n'$, ~~characterized in that~~ in which a set $\underline{s} = (s_0, s_1, ..., s_{n-1})$ of strictly increasing integers, with $s_0 \geq 0$ and $s_{n-1} \leq n'-1$, and a non-singular diagonal matrix B of

dimension n having been predetermined, the method ~~it comprises~~ comprising the ~~following~~ steps of:

[[-]] constructing, on the basis of the information symbols, the polynomial

$$a^B(x) \equiv \sum_{i=m}^{n-1} a_{i-m}\beta_{s_i}^{-1} x^{s_i} ,$$

where β_i is the element of B in position (i, i),

[[-]] implementing steps b), c) and d) of the method according to claim 1, by replacing a(x) with $a^B(x)$, which gives a word $\underline{v}'^B$,

[[-]] deleting the components of predetermined value from $\underline{v}'^B$, which gives a word $\underline{v}^B = (v^B0, v^B1, ..., v^B_{n-1})$, and

[[-]] calculating the word $\underline{v} = (v_0, v_1, ...,v_{n-1})$ defined by: $v_i = v^Bi\beta i$ for all i from 0 to (n-1).

4. (Currently Amended) An encoding method according to any one of the preceding claims, ~~characterized in that~~ in which n' is equal to (q-1) or is a divisor of (q-1), and ~~in that~~ $g(x) = \prod_{i=1}^{m}(x - \alpha^i)$, where α is an element of Fq satisfying $\alpha^{n'} = 1$.

5. (Currently Amended) A method of encoding for algebraic geometric codes, comprising at least one step in which codewords belonging to a shortened [[“MDS”]] MDS linear cyclic code are calculated, ~~characterized in that said~~ in which the calculation is

performed by means of an encoding method according to any one of claims 1 to 3.

6. (Currently Amended) A device [[(102)]] for encoding over a Galois field Fq, where q is an integer greater than 2 and equal to a power of a prime number, in which a word $\underline{v}' = (v'_0, v'_1, \ldots, v'_{n'-1})$ is calculated, where $n' \geq 3$, belonging to an [["MDS"]] linear cyclic code C' of dimension (n'-m), where $1 \leq m \leq n'-2$, on the basis of a word $\underline{a} = (a_0, a_1, \ldots, a_{n-m-1})$ of information symbols, where $m < n < n'$, ~~characterized in that~~ in which, a set $\underline{s} = (s_0, s_1, \ldots, s_{n-i})$ of strictly increasing integers, with $s_0 \geq 0$ and $s_{n-1} \leq n'-1$, having been predetermined, the method comprising the steps of ~~it is adapted to~~:

a) forming the polynomial $a(x) \equiv \sum_{i=m}^{n-1} a_{i-m} x^{s_i}$,

b) ~~calculate~~ calculating the remainder r(x) of the Euclidean division of a(x) by the polynomial $g(x) \equiv \sum_{p=0}^{m} g_p x^p$ generating said code C',

c) ~~calculate~~ calculating the polynomial

$v^*(x) = a(x) - r(x) \equiv \sum_{i=0}^{n'-1} v^*_i \, x^i$, corresponding to the word $\underline{v}^* = (v^*_0, v^*_1, \ldots, v^*_{n'-1})$, and

d) ~~take~~ taking $\underline{v}' = \underline{v}^*$ if $s_{m-i} = m-1$; otherwise to obtain said word $\underline{v}'$ by taking:

$$\underline{v}' = \underline{v}^* + \sum_{j=0}^{s_m-m-1} f_j \underline{\Gamma}^j \qquad (1),$$

in which the words $\underline{\Gamma}^j$ of length n' are defined by: $\Gamma^j_i = g_{i-j}$ for $j \leq i \leq j + m$, and $\Gamma^j_i = 0$ otherwise, and in which the elements f_j of F_q are calculated by means of the equations (1) in which, for the (s_m - m) values of i < s_m not belonging to the set $\underline{s}$, each component v'_i is taken equal to a respective predetermined constant.

7. (Currently Amended) An encoding method according to claim 6, ~~characterized in that~~ in which n' is equal to (q-1) or is a divisor of (q-1), and in that

$g(x) = \prod_{i=1}^{m}(x - \alpha^i)$, where α is an element of Fq satisfying $\alpha^{n'} = 1$.

8. (Currently Amended) An apparatus [[(48)]] for processing data comprising a source of information symbols [[(100)]], ~~characterized in that it further comprises~~ comprising:

[[-]] a storage unit [[(101)]] adapted to accumulate [[said]] the symbols so as to form codewords $\underline{a}$ each containing a predetermined number k of symbols,

[[-]] an encoding device according to claim 6 or claim 7, and

[[-]] a transmitter [[(103)]] adapted to transmit the words $\underline{v}'$ resulting from the encoding of [[said]] the information symbols.

9. (Currently Amended) An apparatus [[(48)]] for processing data comprising a source of information symbols [[(100)]], ~~characterized in that it further comprises~~ comprising:

[[-]] a storage unit [[(101)]] adapted to accumulate [[said]] the symbols so as to form codewords a each containing a predetermined number k of symbols,

[[-]] an encoding device according to claim 6 or claim 7,

[[-]] a shortening unit [[(20)]] adapted to delete said components of predetermined value from v', so as to form a word v of length n , and

[[-]] a transmitter [[(103)]] adapted to transmit the words v resulting from the encoding of [[said]] the information symbols.

10. (Currently Amended) A non-removable data storage means, ~~characterized in that it comprises~~ comprising computer program code instructions for the execution of the steps of an encoding method according to any one of claims 1 to 3.

11. (Currently Amended) A partially or wholly removable data storage means, ~~characterized in that it comprises~~ comprising computer program code instructions for the execution of the steps of an encoding method according to any one of claims 1 to 3.

12. (Currently Amended) A computer program~~, characterized in that it contains~~ containing instructions such that, when said program controls a programmable data processing device, said instructions lead to said data processing device implementing an

encoding method according to any one of claims 1 to 3.

13. (Currently Amended) A method of encoding information by means of a given code shortened in at least one predetermined position, comprising the steps of:

[[-]] dividing a first polynomial representing information symbols by a generator polynomial so as to obtain a remainder polynomial;

[[-]] calculating a second polynomial by subtracting the remainder polynomial from the first polynomial;

[[-]] generating a pre-encoded word belonging to the given code from a sequence of coefficients of the second polynomial, so that the component of the pre-encoded word in the at least one predetermined position has a respective predetermined value; and

[[-]] generating an encoded word by removing from the pre-encoded word the component in the at least one predetermined position.

14. (Currently Amended) A method of encoding for algebraic geometric codes, comprising at least one step in which codewords belonging to a shortened code are calculated, ~~characterized in that~~ in which the calculation of the codewords belonging to the shortened code is performed by using an encoding method according to Claim 13.

15. (Currently Amended) A device for encoding information by means of a given code shortened in at least one predetermined position, comprising:

[[-]] means for dividing a first polynomial representing information symbols by a generator polynomial so as to obtain a remainder polynomial;

[[-]] means for calculating a second polynomial by subtracting the remainder polynomial from the first polynomial;

[[-]] means for generating a pre-encoded word belonging to the given code from a sequence of coefficients of the second polynomial, so that the component of the pre-encoded word in the at least one predetermined position has a respective predetermined value; and

[[-]] means for generating an encoded word by removing from the pre-encoded word the component in the at least one predetermined position.

16. (Original) Information storage medium which can be read by a computer or a microprocessor storing instructions of a computer program for implementing a coding method according to any one of Claims 13 and 14.

17. (Currently Amended) Information storage medium according to Claim 16, ~~characterized in that~~ in which said storage medium is partially or totally removable.

18. (Original) Computer program product comprising sequences of instructions for implementing a coding method according to any of Claims 13 and 14.